

UNITED STATES DISTRICT COURT

for the
District of UtahIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)INFORMATION ASSOCIATED WITH GOOGLE
USER ACCOUNT RASBAND.KEVIN@GMAIL.COM

Case No.

FILED IN UNITED STATES DISTRICT
COURT, DISTRICT OF UTAH
AUG 28 2017 PMW
BY D. MARK JONES, CLERK
2:17mj-00441-PMW
DEPUTY CLERK

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
Google Inc. user account rasband.kevin@gmail.com, more particularly described in Attachment A, which is incorporated by reference herein,

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

Digitally stored information consisting of account user information, location history, device information and history, search and browsing history, services utilized, communications history, information stored by any user of the account, records and session logs, IP history, other subscriber numbers, means and forms of payment and billing records.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
2113(a)	Bank Robbery
924(c)(1)(A)	Using, Carrying and Brandishing a Firearm During and in Relation to a Crime of Violence

The application is based on these facts:

Please see the attached affidavit, which is incorporated by reference herein.

- ☒ Continued on the attached sheet.
☒ Delayed notice of 30 days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

DAVID C. ELKINGTON, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 28 Aug 2017

City and state: Salt Lake City, Utah



Judge's signature

PAUL M. WARNER

Printed name and title

UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH)
OF INFORMATION ASSOCIATED)
WITH THE GOOGLE ACCOUNT)
ASSOCIATED WITH THE)
CELLULAR TELEPHONE NUMBER)
801-678-5841, ELECTRONI SERIAL)
NUMBER 268435457800019448,)
GOOGLE ACCOUNT)
RASBAND.KEVIN@GMAIL.COM,)
AND GOOGLE ID NUMBER)
1340933992864, THAT IS STORED)
AT PREMISES CONTROLLED BY)
GOOGLE, INC.)

~~SEALLED~~

BY ORDER OF THE COURT

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, David C. Elkington, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a Google Account stored at premises controlled by Google, Inc. ("Google"), a provider of electronic communication service, located at 1600 Amphitheater Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government information further

described in Attachment B.

2. I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516. I have been so employed by the Federal Bureau of Investigation (FBI) since 1998. I am currently assigned to the Ogden office of the Salt Lake City Division of the FBI and I am tasked with investigating violent crimes, including bank robbery. As a Special Agent with the FBI, I have participated in investigations involving violent crimes, drug trafficking organizations, counterterrorism, and crimes in the Indian Country. Through my experience in those respective investigative disciplines I have been involved the search, seizure and eventual analysis of electronically stored digital information from electronic storage devices, such as cellular telephones, computers, and removable storage media, as well as the obtaining of related information from supporting electronic infrastructures and service providers, such as cellular telephone companies, internet service providers, and other companies which provide online services via their internet sites or mobile applications. Through my investigative experience I know data is available from such providers and services, and is often of assistance in investigating all nature of criminal activity, including violations of 18 U.S.C. § 2113(a) - Bank Robbery.

3. The statements in this affidavit are based in part on information provided by law enforcement officers assigned to other law enforcement agencies, other Special Agents and employees of the FBI, and on my experience and background as a law enforcement officer and Task Force Officer of the FBI. Since this affidavit is being submitted for the

limited purpose of securing a warrant from the Court, I have not included each and every fact known to me concerning this investigation. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. The United States is investigating the armed bank robbery of the Goldenwest Credit Union, 131 West 200 North, Kaysville, Utah, on February 11, 2017, and the armed bank robbery of the Utah First Credit Union, 1173 North Shepard Creek Parkway, Farmington, Utah, on March 29, 2017. The investigation concerns possible violations of 18 U.S.C. §§ 2113(a) (Bank Robbery) and 924(c)(1)(A) (Using, Carrying and Brandishing a Firearm During and in Relation to a Crime of Violence).

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to search the information described in Attachment A for evidence of armed bank robbery, as further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is a “court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).]

PROBABLE CAUSE

7. On Saturday, February 11, 2017 at approximately 0826 hours, officers with the Kaysville Police Department, Kaysville, Utah, were dispatched to the Goldenwest Credit Union, located at 131 West 200 North, Kaysville, Utah, on report of a bank robbery. Upon their arrival, officers learned that at approximately 0824 hours, two bank employees had arrived and entered the bank at a west-side door. As they entered the bank and the door was closing behind them, an unknown male entered the bank through the same door and confronted the bank employees at gunpoint. The bank employees described the handgun as being small and black. The armed assailant's face was concealed and he was wearing clothing that covered the majority of his body.

8. At gunpoint, the male instructed the two employees to proceed to the bank vault. They complied with his command. The armed man instructed the bank employees to empty the contents of the vault into a bag he supplied to them. They again complied with his demands. When the bank employees had completed emptying the vault, the robber took the bag and exited the bank through the same side door through which he had entered. The robber then fled the immediate area of the bank on foot.

9. On Wednesday, March 29, 2017, at approximately 0803 hours, officers with the Farmington Police Department, located in Farmington, Utah, were dispatched to the Utah First Credit Union, 1173 North Shepard Creek Parkway, Farmington, Utah on report of a bank robbery. Upon their arrival officers learned that at approximately 0740 hours a bank employee with initials S.I. arrived at work. As S.I. made her way into the building

she was confronted at gunpoint by a man who had been hiding in the bushes near the side door. The armed assailant's face was concealed and he was wearing clothing that covered the majority of his body. S.I. described the handgun as being small and black.

10. The robber forced S.I. inside the bank and into the vault. S.I. told the male that—due to a time-based locking system—she would be unable to access the vault for another 15 minutes and that even after that time she would need a second person with proper access rights. The robber told S.I. that he would wait until both conditions were satisfied. The robber ordered S.I. to wait just outside the vault. She was instructed to surrender her phone and sit in silence while they waited.

11. At approximately 0800 hours, a Utah First Credit Union employee with the initials K.M. arrived and entered the building. She was immediately confronted by the robber at gunpoint. K.M. did not have the rights to access the vault and she informed the robber. The robber abandoned his initial plan to access the vault and instead instructed both S.I. and K.M. to open their cash drawers and empty the drawers' contents into a bag. S.I. and K.M. complied, surrendering approximately U.S. currency. Among the cash bundles were two dye packs — both set to detonate once they were carried past an invisible geofence electronically set on the exterior of the credit union property.

12. The robber fled the bank northbound on foot. The dye packs activated and released a significant amount of red dye. The explosions apparently startled the robber because he dropped and abandoned the bag that carried the stolen cash and the gun. Police

later recovered the bag and gun which were covered in the dye from the dye packs. The robber's gun was identified as a RUGER LC9, which is a small, black handgun.

13. On March 29, 2017, Bureau of Alcohol, Tobacco and Firearms (ATF) Special Agent (SA) Tyler Olsen queried the robber's handgun's serial number through the eTrace database. The results suggested that the Ruger handgun had been recently purchased by Kevin RASBAND. The handgun was purchased from CABELA'S, located at 391 North Cabela's Drive, Farmington, Utah. Police confirmed that RASBAND purchased the Ruger handgun from Cabela's on February 8, 2017.

14. On March 29, 2017, FBI Task Force Officer (TFO) Tyler Ziegler queried the Utah Criminal Justice Information System (UCJIS) database for RASBAND's driver's license and motor vehicle information. He discovered RASBAND's listed address showed to 3163 Whitetail Drive, Layton, Utah.

15. On March 29, 2017 TFO T. Ziegler obtained a state Court Order authorizing the receipt of Global Position System (GPS) location information transmitted by RASBAND's cellular telephone. The order was served and location information began delivery by SPRINT on March 29, 2017 at approximately 2100 hours. The receipt of GPS location information served as evidence that the phone in question was on and being serviced by SPRINT on the day the aforementioned robbery was accomplished. The information obtained was not retroactive and did not provide information about the device's location prior to service

16. On March 31, 2017, a search of RASBAND's cellular telephone was executed by law enforcement officers of the Kaysville Police Department, Kaysville, Utah, and the Farmington Police Department, Farmington, Utah pursuant to a search warrant issued by the State of Utah. The subject cellular telephone was obtained by law enforcement officers from RASBAND's wife, who reported she had received it from her husband prior his arrest on state criminal charges on March 30, 2017. The search of the telephone indicated the telephone was an HTC PG86100 Evo 3D model utilizing the Google Android operating system. The Android ID number was identified as 5e4170f15dc21daa, the Google ID number was 1340933992864, the associated Google account was rasband.kevin@gmail.com, the detected telephone number was (801) 678-5841, the ISMI was 31000801280644l, the Electronic Serial Number (ESN) was 268435457800019448, and the service provider was SPRINT, and

17. On May 3, 2017, a grand jury for the District of Utah returned an indictment on RASBAND charging him with the robbery of both credit unions and the brandishing of a gun during each incident.

18. Based on what I have learned about Google, Inc. and the services it provides, I believe Google can provide GPS data, cell site/cell tower information and Wi-Fi access points for RASBAND's telephone. I believe this data will show the movements of RASBAND's telephone before, during and after the reported bank robberies on February 11, 2017, and March 29, 2017. Furthermore, in the event RASBAND was not using the exact cellular telephone device which was searched on March 31, 2017, but

rather was using an unknown telephone but was still signed-in to his Google account of rasband.kevin@gmail.com on the device, Google may still be able to provide some or all of the aforementioned data.

BACKGROUND CONCERNING GOOGLE ACCOUNT INFORMATION

19. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

20. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and

experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

21. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, email providers typically log the IP addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Lastly, stored electronic data may provide relevant insight into the email

account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

22. According to representatives of Google, the company keeps records that can reveal Google accounts accessed from the same electronic device, such as the same computer or mobile phone, including accounts that are linked by "cookies," which are small pieces of text sent to the user's Internet browser when visiting websites. This warrant requires Google to identify any other accounts accessed by the same device(s) that accessed the Subject Account described in Attachment A, including accounts linked by cookies, recovery email address, or telephone number. This warrant will ask that Google identify such accounts and produce associated subscriber information (not content).

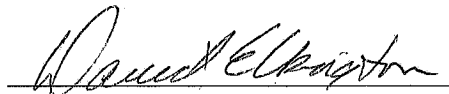
23. In my training and experience, I have learned that Google collects and retains location data from Android enabled mobile devices. The company uses this information for location based advertising and location based search results. Per Google, this information is derived from GPS data, cell site/cell tower information, and Wi-Fi access points. While the specific parameters of when this data is collected are not entirely clear, it appears that Google collects this data whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text messages, internet access, or e-mail access.

24. I believe this data will show the movements of Kevin Dean RASBAND's mobile devices during the relevant period of each robbery. I also believe this data will assist investigators with establishing patterns of movement by RASBAND as he took preparatory steps and formulated plans to rob each financial institution, such as casing the banks to gather information about the bank employees and bank operations.

CONCLUSION

25. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

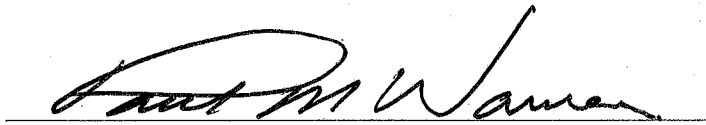


DAVID C. ELKINGTON

Special Agent

Federal Bureau of Investigation

Subscribed and sworn to before me on Aug 28, 2017



PAUL M. WARNER

UNITED STATES CHIEF MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

Information from the Google Account associated with the suspect account that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered in Mountain View, California, is as follows:

- Google account rasband.kevin@gmail.com;
AND/OR,
- Cellular telephone number 801-678-5841;
AND/OR,
- Android device assigned ESN 268435457800019448;
AND/OR,
- Google ID 1340933992864;
AND/OR,
- Android ID 5e4170f15dc21daa.

ATTACHMENT B

Particular Things to be Seized

Location History: All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings from the time periods: January 28, 2017 through February 12, 2017; and March 20, 2017 through March 30, 2017.

- a. All records or other information regarding the identification of the account subscriber and/or user(s), to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, login IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- b. All device information associated with the account;
- c. All location history associated with the account;
- d. All search and browsing history associated with the account;
- e. The types of service utilized;

f. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

g. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

h. For all Google accounts that are linked to any of the accounts listed in Attachment A by cookies, recovery email address, or telephone number, provide:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses);
3. Local and long distance telephone connection records;
4. Records of session times and durations and IP history log;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), MSISDN, International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Station Equipment Identities ("IMEI"));

7. Other subscriber numbers or identities (including temporarily assigned network addresses and registration IP addresses (including carrier grade natting addresses or ports)); and
8. Means and source of payment for such service (including any credit card or bank account number) and billing records.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL
RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, Inc., and my official title is _____. I am a custodian of records for Google. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google; and
- c. such records were made by Google as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature